Defining Electronic Warfare

Electronic Warfare (EW) is the use of the electromagnetic spectrum to effectively deny its use by an adversary, while optimizing its use by friendly forces. Electronic warfare has three main components: electronic attack; electronic protection; and, electronic support.

- **Electronic Attack (EA)** is the active or passive use of the electromagnetic spectrum to deny its use by an adversary. "Active EA" includes such activities as the use of chaff, balloons, radar reflectors, Faraday cages, winged decoys, and other stealth devices or techniques.
- **Electronic Protection (EP)** includes all activities related to making enemy EA activities less successful by protecting friendly personnel, facilities, equipment or objectives. EP can also be implemented to prevent friendly forces from being affected by their own EA. "Active EP" includes such activities as technical modifications to radio equipment. Passive EP includes such activities as the education of operators and modified battlefield tactics or operations.
- **Electronic Support (ES)** is the use of the electromagnetic spectrum to gain intelligence about other parties on the battlefield in order to find, identify, locate and intercept potential threats or targets. This intelligence, known as ELINT, might be used by fire-control systems for artillery or airstrike orders, for mobilization of friendly forces to a specific location or objective on the battlefield, or as the basis of electronic attack or electronic protection actions.

Organization

CAC-CDID develops and integrates CNO and EW capabilities for the USACAC. To accomplish this task, CNO and EW expertise is distributed among CAC-CDID's following Divisions: Concepts Development Division (CDD), Requirements Determination Division (RDD), Battle Command Battle Lab (BCBL), TRADOC Capabilities Manager Computer Network Operations and Electronic Warfare (TCM-CEW) and TCM–Battle Command (TCM-BC).

From an undeveloped, initial idea, the Concepts Development Division develops the context for assessment and analysis which is necessary to start the capability development process. This analysis is then transferred to the Requirements Determination Division which defines the requirements for CNO and EW capabilities and recommends the necessary DOTMLPF solutions. Through rigorous experimentation and prototyping, the Battle Command Battle Lab tests these solutions to ensure proper integration into the warfighting of commanders and staffs. The TCM-CEW is CAC-CDID's interface with the Warfighter. They continually communicate with soldiers in the field and provide the necessary synchronization and monitoring of CNO and EW capabilities to keep the Warfighter well equipped to meet current and future challenges. Additionally, CDID's TCM-BC also integrates CNO and EW related requirements for Unified Battle Command (UBC) in support of Battle Command/ Network Segments of the LandWarNet Capability Set Development.

A goal for CAC-CDID is to build a Community of Practice where members routinely coordinate on a shared vision for Cyberspace, and the broader electromagnetic spectrum (EMS). This partnership will enable a broad range of interaction between our joint partners, interagency partners, intergovernmental partners, multinational partners, the academician, the industrialist, and the Soldier; allowing for and promoting the reduction of risk to Land Component Forces.

CAC-CDID is embarking on an effort to work with the universities in the Great Plains on development and research initiatives that will benefit both the Army and the students/faculty involved. Army Research Labs staffs out development projects to Academics for the purpose of designing technologies to save Soldiers lives. Our goal is to ensure that the Big 12, our homegrown Universities, are strong participants and reap the benefits of helping to keep us "Army Strong."

We are also working on a partnership with the United States Marine Corps. This partnership would mean all members of the Land Force would be working together towards mutual goals in the Cyber Space and EMS. This will establish personal relationships enabling the development of well-coordinated solutions through a land lens, recognizing the land domain is host to the most complex factor of all, people.

Finally, we are initiating relationships with several industry partners to further our understanding of developments in mass-market computers, networks and electronics.

For more information on this capability development area, contact the Capability Development Integration Directorate at: 806 Harrison Ave, Fort Leavenworth, Kansas 66027 (913) 684-5175, or visit their Web site at http://usacac.army.mil/cac2/cdid/index.asp

Capability Development Integration Directorate (CDID) Development Area: Computer Network Operations and Electronic Warfare

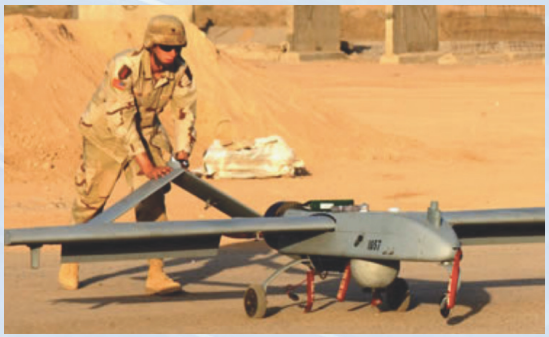
CDID

U.S. Army Combined Arms Center

"Intellectual Center of the Army"

Background

The electromagnetic spectrum (EMS) has been used for military applications for more than a century. Today, use of the EMS reaches far beyond radio communications into the realm of sophisticated technologies such as high power microwaves and directed energy weapons. These developments coincide with similar advances in computer network technology and activities in cyberspace. Such technological advances have diminished the size and cost of potentially dangerous capabilities, thus making them both more affordable as well as more portable.



One consequence is that much of modern EMS technology is readily available to our current, as well as potential, adversaries, from off-the-shelf civilian sources. For example, cellular and satellite communications are now commonplace. As a land force, the Army operates in and among populaces that are increasingly connected by computers, telecommunications systems and electronic devices. Such developments guarantee that the EMS in which our own military forces will operate will become more complex, challenging and dangerous.

Moreover, the increasing convergence of computer network operations and electronic warfare capabilities will likely produce unexpected new battlefield challenges. In the face of such current and future threats, Army forces must gain the capability to dominate the EMS and cyberspace in the same way they have dominated traditional land warfare domains of the past. Consequently, it is imperative that commanders gain unimpeded access to and use of cyberspace and the EMS as needed to conduct Computer Network Operations (CNO) and Electronic Warfare (EW). To support the Army in developing the necessary dominance in these areas, it must be adaptive and aggressive in defining concepts and building capabilities aimed at successfully developing and employing CNO and EW across the full spectrum of operations.

Army Proponent

The U.S. Army Combined Arms Center (USACAC) is the Army's proponent for CNO and EW. The Capability Development Integration Directorate (CDID) is the organization that develops and manages these capabilities for CAC to deal with current and future threats. Its mission with regard to CNO and EW is to develop, synchronize, integrate and coordinate Computer Network Operations and Electronic Warfare (CNO-EW) capabilities and capacity across the Doctrine, Organization, Training, Material, Leadership and Education, Personnel and Facilities (DOTMLPF) domains in order to prepare the Army and the Land Component for future challenges in the EMS and cyberspace.

CNO-EW Way Ahead

Full integration of computer network operations and electronic warfare capabilities into the broader Army to ensure that cyberspace and the broader electromagnetic spectrum (EMS) are optimally exploited by Soldiers and leaders who understand both the operational and technical dimensions of this segment of the operational environment to enable a broad range of joint, interagency, intergovernmental and multinational activities during full spectrum operations while concurrently reducing risk to the force. To achieve this vision, the following are necessary:

- Synchronize, integrate and coordinate CNO and EW with modularity and future requirements.
- Develop CNO and EW Doctrine, Organizations, Training, Material, Leadership, Personnel and Facilities (DOTMLPF) requirements.
- Determine the scope of future CNO and EW capabilities development efforts.
- Determine integration tasks for Army, Joint, Interagency, Intergovernmental and Multinational computer network and electronic warfare operations.

- Perform as the Army's centralized manager and integrator for CNO and EW combat development and force management activities.

Defining Computer Network Operations

Computer Network Operations (CNO) originate from the increasing use of networked computers and supporting IT infrastructure systems by military and civilian organizations. For the purpose of military operations, CNO are divided into computer network attack (CNA), computer network defense (CND), and related computer network exploitation (CNE) enabling operations.

- **Computer Network Attack (CNA)** uses computer networks to disrupt, deny, degrade or destroy the information within adversary computers and computer networks, or the computers and supporting automated data processing systems themselves.
- **Computer Network Defense (CND)** uses computer networks to protect, monitor, analyze, detect and respond to network attacks, intrusions, disruptions or other unauthorized actions that would compromise or cripple defense information systems and networks.
- **Computer Network Exploitation (CNE)** uses computer networks to collect intelligence from enemy information systems or networks.